

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-165377
 (43)Date of publication of application : 16.06.2000

(51)Int.Cl.

H04L 9/14
 G06F 13/00
 G09C 1/00
 H04L 9/32

(21)Application number : 10-340635

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 30.11.1998

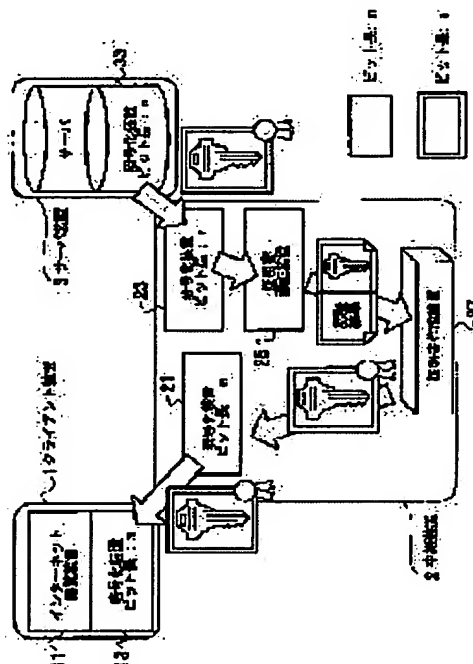
(72)Inventor : FUKAZAWA HIROAKI
 MOTODA TOSHIHIRO

(54) ENCRYPTION PROTOCOL CONVERTER, ENCRYPTION PROTOCOL CONVERTING METHOD AND RECORDING MEDIUM RECORDING ENCRYPTION PROTOCOL CONVERSION PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an encryption protocol converter that enhances security for information transmission reception furthermore and can precisely authenticate a communication opposite party, and to provide an encryption protocol conversing method and a recording medium recording an encryption protocol conversion program.

SOLUTION: Encryption devices 21, 23 of an intermediate device 2 encrypt furthermore encrypted information sent/received between a client device 1 and a server device 3 so as to enhance the security, and a certificate authentication device 25 of the intermediate device 2 authenticates a certificate added to the encrypted information received from the server device 3, a certificate generator 27 generates a new certificate on the basis of the authentication result and the generated certificate is transmitted to the client device 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-165377

(P2000-165377A)

(43) 公開日 平成12年6月16日 (2000.6.16)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 J 1 0 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 9 A 0 0 1
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 Z

審査請求 未請求 請求項の数 6 O L (全 18 頁)

(21) 出願番号 特願平10-340635

(22) 出願日 平成10年11月30日 (1998. 11. 30)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 深澤 広明

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 元田 敏浩

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100083806

弁理士 三好 秀和 (外1名)

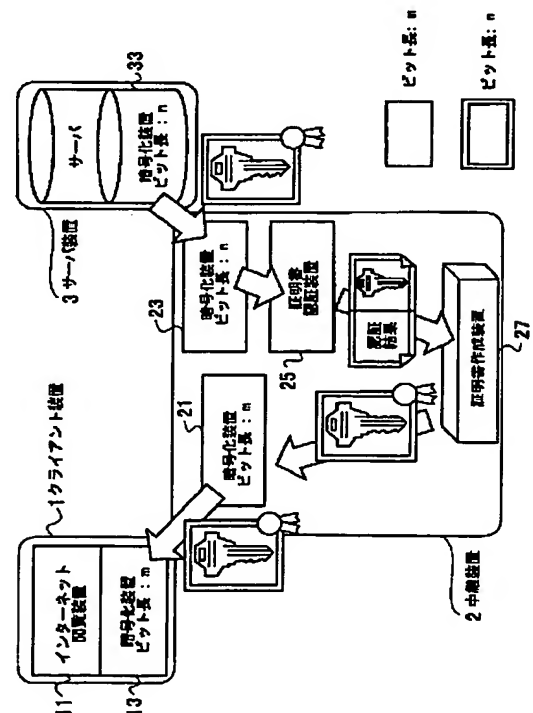
最終頁に続く

(54) 【発明の名称】 暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体

(57) 【要約】

【課題】 情報の送受信におけるセキュリティを更に強化するとともに通信相手を適確に認証し得る暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体を提供する。

【解決手段】 クライアント装置1とサーバ装置3との間で授受される暗号化情報を中間装置2の暗号化装置21、23で更に暗号化しセキュリティを強化するとともに、中間装置2においてサーバ装置3から受信した暗号化情報に付加されている証明書を証明書認証装置25で認証し、この認証結果に基づき証明書作成装置27で新たに証明書を作成し、この作成された証明書をクライアント装置1に送信する。



【特許請求の範囲】

【請求項1】 クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換装置であって、
クライアント装置とサーバ装置との間に設けられる中間装置を有し、該中間装置は、
クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信する第1の暗号化手段と、
サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信する第2の暗号化手段と、
サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証する証明書認証手段と、
該証明書認証手段の認証結果に基づき新たに証明書を作成する証明書作成手段と、
該証明書作成手段で作成された証明書を前記第2の暗号化手段で暗号化してクライアント装置に送信する送信手段とを有し、
クライアント装置は、前記認証鍵と同じ認証鍵を有し、
該認証鍵で前記中間装置から送信されてくる証明書を認証する認証手段を有することを特徴とする暗号プロトコル変換装置。

【請求項2】 前記証明書作成手段で新たに作成された証明書を保存する証明書保存手段と、
前記証明書認証手段での認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第2の暗号化手段で暗号化してクライアント装置に返送する返送手段とを更に有することを特徴とする請求項1記載の暗号プロトコル変換装置。

【請求項3】 クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換方法であって、
クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、
サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、
サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、
この認証結果に基づき新たに証明書を作成し、
この作成された証明書を暗号化してクライアント装置に送信し、
クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証することを特徴とする暗号プロトコル変換方法。

【請求項4】 前記新たに作成された証明書を証明書保存手段に保存し、
前記認証結果に基づき前記証明書保存手段から証明書を

検索し、この検索した証明書を暗号化してクライアント装置に返送することを特徴とする請求項3記載の暗号プロトコル変換方法。

【請求項5】 クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換プログラムを記録した記録媒体であって、
クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、
サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、
サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、
この認証結果に基づき新たに証明書を作成し、
この作成された証明書を暗号化してクライアント装置に送信し、

クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証することを特徴とする暗号プロトコル変換プログラムを記録した記録媒体。

【請求項6】 前記新たに作成された証明書を証明書保存手段に保存し、
前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を暗号化してクライアント装置に返送することを特徴とする請求項5記載の暗号プロトコル変換プログラムを記録した記録媒体。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、インターネットやイントラネットに代表されるWWWシステムのサーバ装置において情報を提示する際のセキュリティを強化する暗号プロトコル変換装置および方法に関し、更に詳しくは、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】 インターネットやイントラネット等のネットワークを介したクライアント装置とサーバ装置との間における情報の送受信においては、従来、例えば図19に示すように、クライアント装置1のインターネット閲覧装置11に付随する暗号化装置13によってクライアント装置1からの要求情報を暗号化し、そのままサーバ装置3に送信し、またサーバ装置3においても暗号化装置33で応答情報を暗号化し、同様にそのまま送信している。このような構成は単純であるが、セキュリティが弱いので重要な情報の送受信には不安がある。なお、図19において、鍵マークは、暗号化された情報を示している。

【0003】 また、この例では、クライアント装置1の

暗号化装置13でサポートしているビット長は m ビットであり、サーバ装置3の暗号化装置33でサポートしているビット長は n ビットであって、両者の関係は $m < n$ であり、ビット長は合ってなく、クライアント装置1の暗号化装置13は短いビットで構成されているため、十分な安全性を保てない危険性がある。

【0004】また、従来別の例として、図20および図21に示すように、クライアント装置1とサーバ装置3との間にビット長 m をサポートする第1の暗号化装置51とビット長 n をサポートする第2の暗号化装置53を有する中間装置5を設け、この中間装置5でクライアント装置1とサーバ装置3との間の情報を暗号化してセキュリティを更に強化するものがある。

【0005】このように構成される従来例では、クライアント装置1において暗号化装置13で暗号化された要求情報は、図20に示すように、中間装置5の暗号化装置51、53でビット長 n に変換されて暗号化され、サーバ装置3に送信され、これによりセキュリティを強化している。

【0006】また、サーバ装置3において暗号化装置33で暗号化され、証明書を付加された応答情報は、図21に示すように、中間装置5の暗号化装置51、53でビット長 m に変換されて暗号化されて、クライアント装置1に送信され、これによりセキュリティを強化しているが、この場合に前記応答情報は中間装置5で認証されるため、中間装置からクライアント装置へ渡る応答情報は証明書が付加されていない状態にある。従って、クライアント装置が受け取る応答情報の発信元を特定することはできない。

【0007】なお、図21において、鍵マークは暗号化された情報を示し、記章マークは証明書付きであることを示している。

【0008】また、図22に示すように、一般に流通しているインターネット閲覧装置11を有するクライアント装置1の暗号化装置13がサポートするビット長が m ビットであって、サーバ装置3の暗号化装置33がサポートするビット長 n と合わない場合には、クライアント装置1の暗号化装置13をビット長 n をサポートする暗号化装置130に取り替える方法もある。

【0009】

【発明が解決しようとする課題】上述した従来技術において、図19で示す方法はセキュリティが弱く、重要な情報の送受信に不安があり、十分な安全性を保つことができないという問題がある。

【0010】また、図20、図22で示す従来技術において、セキュリティの問題は解消し得るが、サーバ装置3から中間装置5へ情報を送信する際、中間装置5で証明書の認証を行ってしまい、クライアント装置1には証明書が送信されないため、クライアント装置1では証明書の認証を行うことができず、従って通信の相手を認証

できず、誤った情報がクライアント装置1に送られてもクライアント装置1の方で認証できないという問題がある。

【0011】本発明は、上記に鑑みてなされたもので、その目的とするところは、情報の送受信におけるセキュリティを更に強化するとともに通信相手を適確に認証し得る暗号プロトコル変換装置および方法と暗号プロトコル変換プログラムを記録した記録媒体を提供することにある。

【0012】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換装置であって、クライアント装置とサーバ装置との間に設けられる中間装置を有し、該中間装置は、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信する第1の暗号化手段と、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信する第2の暗号化手段と、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証する証明書認証手段と、該証明書認証手段の認証結果に基づき新たに証明書を作成する証明書作成手段と、該証明書作成手段で作成された証明書を前記第2の暗号化手段で暗号化してクライアント装置に送信する送信手段とを有し、クライアント装置は、前記認証鍵と同じ認証鍵を有し、該認証鍵で前記中間装置から送信されてくる証明書を認証する認証手段を有することを要旨とする。なお、前記送信手段にあつては、証明書作成手段で作成された証明書をサーバ装置から受信した暗号化情報に付加し、この証明書を付加された暗号化情報を更に前記第2の暗号化手段で暗号化してクライアント装置に送信するものであっても良い。

【0013】請求項1記載の本発明にあつては、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信するため、セキュリティが更に強化されるとともに、クライアント装置は通信相手を適確に認証することができる。

【0014】また、請求項2記載の本発明は、請求項1記載の発明において、前記証明書作成手段で新たに作成された証明書を保存する証明書保存手段と、前記証明書認証手段での認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第2の暗号

化手段で暗号化してクライアント装置に返送する返送手段とを更に有することを要旨とする。なお、前記返送手段にあっては、サーバ装置から受信した暗号化情報に対して付加された証明書を中間装置が認識した結果を前記証明書保存手段から検索し、この検索した結果、以前作成された証明書が存在するときには、前記証明書作成手段で新たな証明書を作成することなく、前記証明書保存手段に保存されている証明書を暗号化情報に付加し、前記第2の暗号化手段で暗号化してクライアント装置に返送するものであっても良い。

【0015】請求項2記載の本発明にあっては、新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第2の暗号化手段で暗号化してクライアント装置に返送するため、2回目以降の接続ではサーバ装置からの証明書を認証した後、証明書を新たに作成する必要がなく、通信速度が速くなり、通信時間を短縮することができる。

【0016】更に、請求項3記載の本発明は、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換方法であって、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信し、クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証することを要旨とする。なお、前記作成された証明書を暗号化してクライアント装置に送信する際に、該証明書をサーバ装置から受信した暗号化情報に付加し、この証明書を付加された暗号化情報をさらに暗号化してクライアント装置に送信するようにしても良い。

【0017】請求項3記載の本発明にあっては、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信するため、セキュリティが更に強化されるとともに、クライアント装置は通信相手を適確に認証することができる。

【0018】請求項4記載の本発明は、請求項3記載の発明において、前記新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存

手段から証明書を検索し、この検索した証明書を暗号化してクライアント装置に返送することを要旨とする。なお、証明書を暗号化してクライアント装置に返送する際に、サーバ装置から受信した暗号化情報に対して付加された証明書を中間装置が認識した結果を前記証明書保存手段から検索し、この検索した結果、以前作成された証明書が存在するときには、新たな証明書を作成することなく、証明書保存手段に保存されている証明書を暗号化情報に付加し、前記第2の暗号化手段で暗号化してクライアント装置に返送するようにしても良い。

【0019】請求項4記載の本発明にあっては、新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第2の暗号化手段で暗号化してクライアント装置に返送するため、2回目以降の接続ではサーバ装置からの証明書を認証した後、証明書を新たに作成する必要がなく、通信速度が速くなり、通信時間を短縮することができる。

【0020】また、請求項5記載の本発明は、クライアント装置とサーバ装置との間においてネットワークを介して送受信される暗号化情報のセキュリティを強化する暗号プロトコル変換プログラムを記録した記録媒体であって、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信し、クライアント装置は、この送信されてくる証明書を受信し、前記認証鍵と同じ認証鍵で認証する暗号プロトコル変換プログラムを記録媒体に記録することを要旨とする。なお、前記作成された証明書を暗号化してクライアント装置に送信する際に、該証明書をサーバ装置から受信した暗号化情報に付加し、この証明書を付加された暗号化情報をさらに暗号化してクライアント装置に送信するようにしても良い。

【0021】請求項5記載の本発明にあっては、クライアント装置から受信した暗号化情報を更に暗号化しセキュリティを強化してサーバ装置に送信し、サーバ装置から受信した暗号化情報を更に暗号化しセキュリティを強化してクライアント装置に送信し、サーバ装置から受信した暗号化情報に付加されている証明書を認証鍵で認証し、この認証結果に基づき新たに証明書を作成し、この作成された証明書を暗号化してクライアント装置に送信する暗号プロトコル変換プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0022】更に、請求項6記載の本発明は、請求項5記載の発明において、前記新たに作成された証明書を証

明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を暗号化してクライアント装置に返送する暗号プロトコル変換プログラムを記録媒体に記録することを要旨とする。

【0023】請求項6記載の本発明にあつては、新たに作成された証明書を証明書保存手段に保存し、前記認証結果に基づき前記証明書保存手段から証明書を検索し、この検索した証明書を前記第2の暗号化手段で暗号化してクライアント装置に返送する暗号プロトコル変換プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。なお、証明書を暗号化してクライアント装置に返送する際に、サーバ装置から受信した暗号化情報に対して付加された証明書を中間装置が認識した結果を前記証明書保存手段から検索し、この検索した結果、以前作成された証明書が存在するときには、新たな証明書を作成することなく、証明書保存手段に保存されている証明書を暗号化情報に付加し、前記第2の暗号化手段で暗号化してクライアント装置に返送するようにしても良い。

【0024】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図1は、本発明の一実施形態に係る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図である。同図に示す暗号プロトコル変換装置は、クライアント装置1とサーバ装置3との間においてインターネットやイントラネット等のネットワークを介して送受信される暗号化情報のセキュリティを強化するために、クライアント装置1とサーバ装置3との間に設けられた中間装置2を有する。

【0025】中間装置2は、クライアント装置1側に設けられ、クライアント装置1の暗号化装置13がサポートするビット長 m に対応するビット長 n をサポートする第1の暗号化装置21、サーバ装置3側に設けられ、クライアント装置1の暗号化装置13がサポートするビット長 n に対応するビット長 m をサポートする第2の暗号化装置23、クライアント装置1から受信した暗号化情報に付加されている証明書を認証する証明書認証装置25、およびこの認証結果に基づき新たに証明書を作成する証明書作成装置27を有する。

【0026】なお、前記第1および第2の暗号化装置13、23がサポートするビット長 m 、 n の関係は $m < n$ であり、クライアント装置1の暗号化装置13は短いビットで構成されているものであるが、本発明は、これに限定されるものではなく、逆に $m > n$ の場合にも同様に適用し得るものである。また、図1において、鍵マークは暗号化された情報を示し、記章マークは証明書付きであることを示している。

【0027】次に、このように構成される実施形態の作用について図2～図11に示すシーケンスチャートを参

照して説明する。なお、図2は図3～図11に示す一連のシーケンスを1つにまとめたものであり、その内容は図3～図11に逐次説明するものと同じであるので、以下の説明では図3～図11に従って順に説明するが、この場合に図2のまとめたシーケンスも参照されたい。

【0028】まず、図3に示すように、クライアント装置1はサーバ装置3への要求情報を中間装置2に送信すると同時にサーバ装置3への証明書の発行要求情報を中間装置2に送信する。

【0029】中間装置2は、図4に示すように、クライアント装置1から送信されてきた要求情報および証明書発行要求情報を受信すると、第1の暗号化装置21および第2の暗号化装置23を使用して、更に高度な暗号化処理を行う。それから、中間装置2は、図5に示すように、この暗号化された要求情報および証明書発行要求情報をサーバ装置3に送信する。

【0030】サーバ装置3は、図6に示すように、前記要求情報および証明書発行要求情報を受信すると、これらの要求に基づいて応答情報を証明書付きで中間装置2に送信する。

【0031】中間装置2は、図7に示すように、前記証明書付き応答情報を受信すると、該情報を証明書認証装置25に送る。証明書認証装置25は、該応答情報に付加されている証明書を認証鍵で認証し、この認証結果を図8に示すように証明書作成装置27に供給する。

【0032】証明書作成装置27は、証明書認証装置25からの認証結果を受け取ると、該認証結果に基づき図9に示すように新たに証明書を作成する。この新たに作成された証明書を付けた応答情報に対して第1の暗号化装置21および第2の暗号化装置23で更に高度な暗号化処理を行い、図10に示すように、中間装置2からクライアント装置1に返送する。

【0033】クライアント装置1は、中間装置2から証明書付き応答情報を受信すると、中間装置2の認証鍵と同じ認証鍵を使用して、証明書を認証し、この認証結果に基づき応答情報をインターネット閲覧装置11に供給して表示する。この際、認証に失敗した場合には、インターネット閲覧装置11は警告を発生する。また、上述した処理において、万が一にも要求した内容と異なった証明書を中間装置2が受け取った場合でも、中間装置2は従来作成される証明書と全く異なった証明書を発行することにより、クライアント装置1で認証する際、警告を発生し誤った情報を受け取ることを防止することができる。

【0034】その後は、図11に示すように、クライアント装置1からの要求情報とサーバ装置3から応答情報の授受が中間装置2の第1の暗号化装置21および第2の暗号化装置23を介して繰り返される。

【0035】次に、本発明の他の実施形態について図12を参照視して説明する。図12は、他の実施形態に係

る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図であり、同図に示す暗号プロトコル変換装置は、図1に示した実施形態に対して証明書保存装置29を追加し、これにより証明書保存装置29で新たに作成した証明書を保存しておき、証明書認証装置25の認証結果に基づき該証明書保存装置29から証明書を検索し、この検索した証明書をクライアント装置1に返送することにより新たな証明書を発行する手間を省略し、通信時間を短縮するようにしたものである。

【0036】このように構成される実施形態の作用について図13～図18に示すシーケンスチャートを参照して説明する。なお、図13は図14～図18に示す一連のシーケンスを1つにまとめたものであり、その内容は図14～図18に逐次説明するものと同じであるので、以下の説明では図14～図18に従って順に説明するが、この場合に図13のまとめたシーケンスも参照されたい。

【0037】また、本実施形態の作用のうち、クライアント装置1から情報を送信し、サーバ装置3から証明書付き応答情報を中間装置2に送信するまでの処理は、上述した図3～図6に示す処理と同じであり、その説明は省略して、その続きについて図14以降を参照して説明する。

【0038】すなわち、中間装置2は、サーバ装置3から証明書付き応答情報を受信すると、図14に示すように、該情報を証明書認証装置25に送る。証明書認証装置25は、該応答情報に付加されている証明書を認証鍵で認証し、この認証結果を図15に示すように証明書保存装置29に供給する。

【0039】証明書保存装置29は、図16に示すように、証明書の認証結果から以前に証明書作成装置27で作成されたサーバ装置3に関する証明書を検索する。そして、この検索した証明書を付加した応答情報に対して第1の暗号化装置21および第2の暗号化装置23で更に高度の暗号化処理を行い、図17に示すようにクライアント装置1に返送する。

【0040】その後は、図18に示すように、クライアント装置1からの要求情報とサーバ装置3から応答情報の授受が中間装置2の第1の暗号化装置21および第2の暗号化装置23を介して繰り返される。

【0041】

【発明の効果】以上説明したように、本発明によれば、クライアント装置とサーバ装置との間で授受される暗号化情報に対して更に高度の暗号化処理を施すとともに、サーバ装置からの暗号化情報に付加されている証明書を認証し、該認証結果に基づき新たに証明書を作成し、この証明書を暗号化してクライアント装置に送信するので、セキュリティが更に強化され、安全性を向上することができるとともに、クライアント装置は通信相手を適確に認証することができる。

【0042】また、本発明によれば、新たに作成された証明書を証明書保存手段に保存し、認証結果に基づき証明書保存手段から証明書を検索し、この証明書をクライアント装置に返送するので、2回目以降の接続ではサーバ装置からの証明書を認証した後、証明書を新たに作成する必要がなく、通信速度が速くなり、通信時間を短縮することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図である。

【図2】図1に示す暗号プロトコル変換装置の全体的作用を示すシーケンス図である。

【図3】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図4】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図5】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図6】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図7】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図8】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図9】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図10】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図11】図1に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図12】本発明の他の実施形態に係る暗号プロトコル変換方法を実施する暗号プロトコル変換装置の構成を示す図である。

【図13】図2に示す暗号プロトコル変換装置の全体的作用を示すシーケンス図である。

【図14】図2に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図15】図2に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図16】図2に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図17】図2に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図18】図2に示す暗号プロトコル変換装置の処理の一部を示すシーケンス図である。

【図19】従来技術におけるクライアント装置とサーバ装置との間における情報の送受信の一例を説明するための図である。

【図20】従来技術におけるクライアント装置とサーバ

装置との間における情報の送受信の他の例を説明するための図である。

【図21】図20の従来技術におけるサーバ装置からクライアント装置への情報の送信を示す図である。

【図22】従来技術の別の例を示す図である。

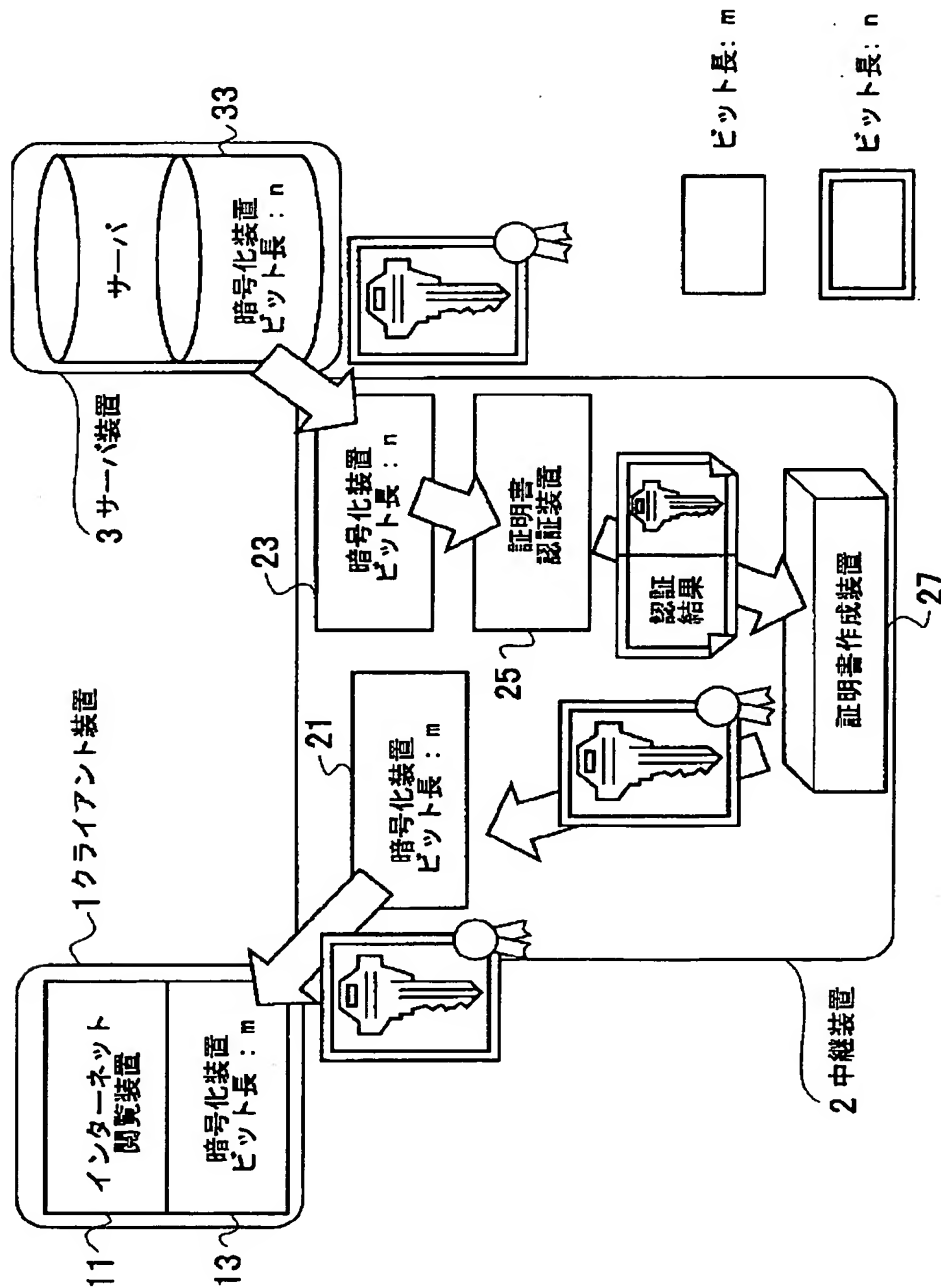
【符号の説明】

- 1 クライアント装置
2 中間装置

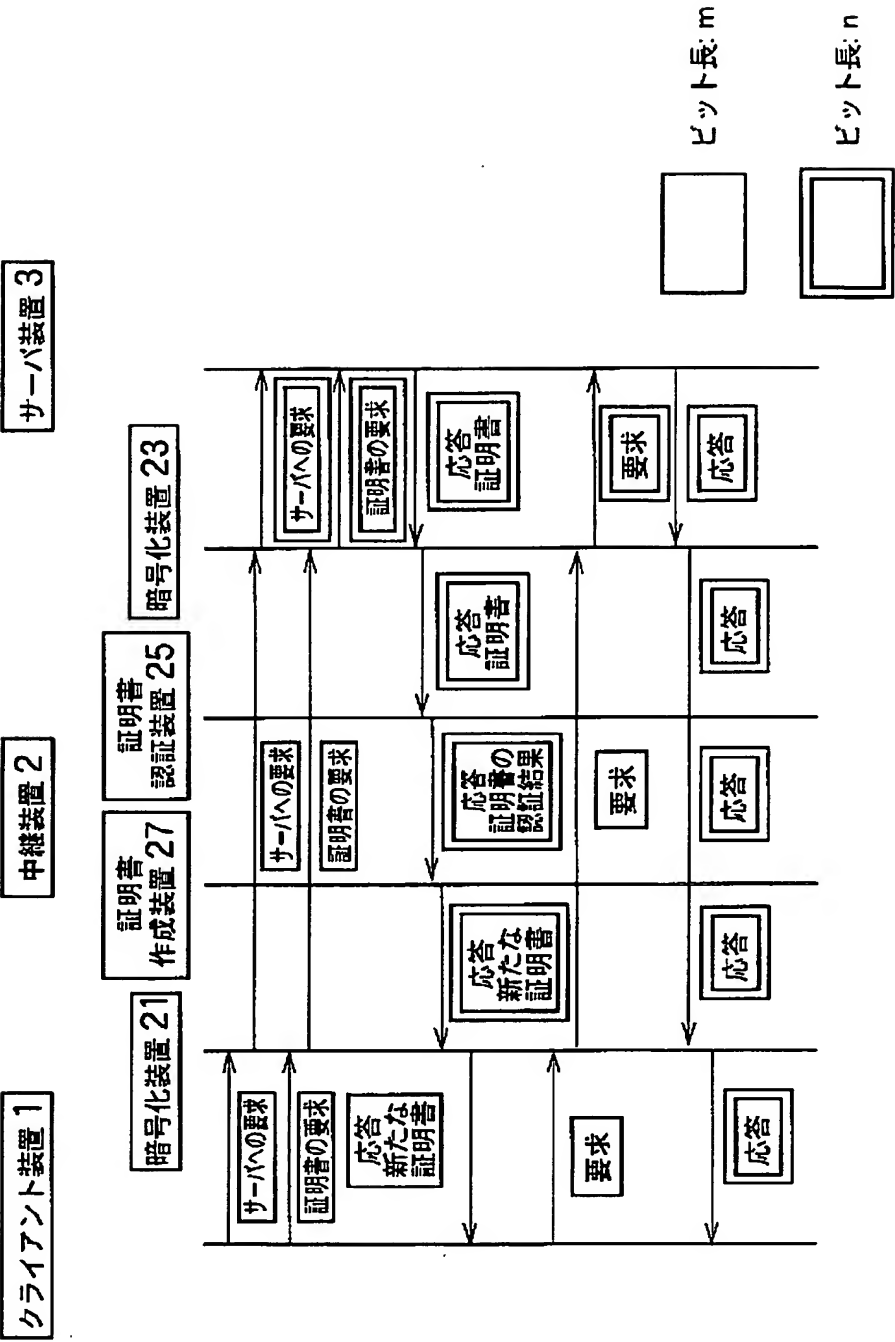
3 サーバ装置

- 11 インターネット閲覧装置
13, 33 暗号化装置
21 第1の暗号化装置
23 第2の暗号化装置
25 証明書認証装置
27 証明書作成装置
29 証明書保存装置

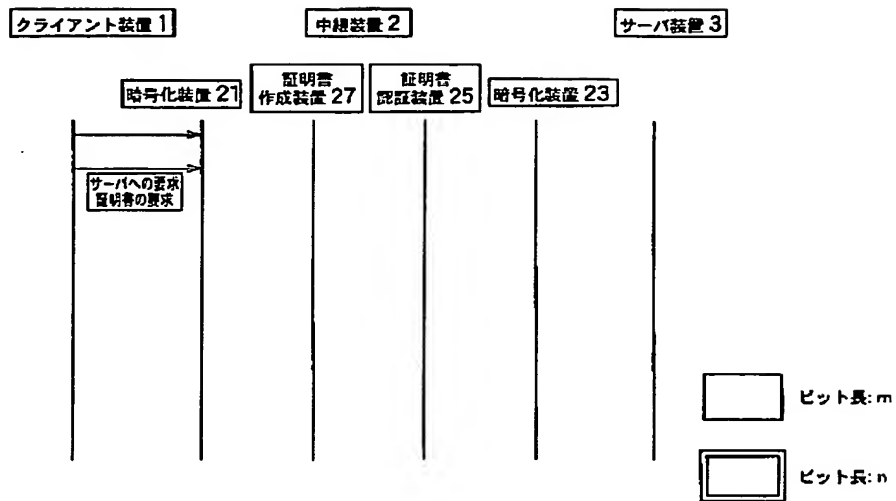
【図1】



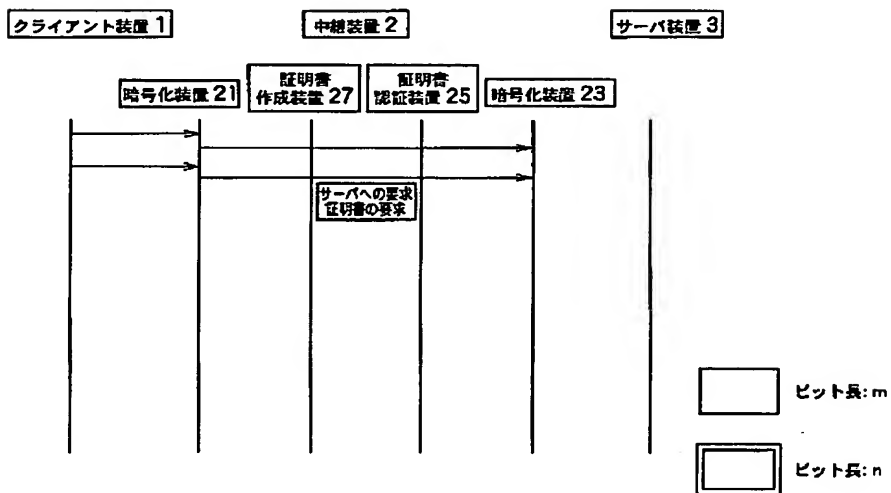
【図2】



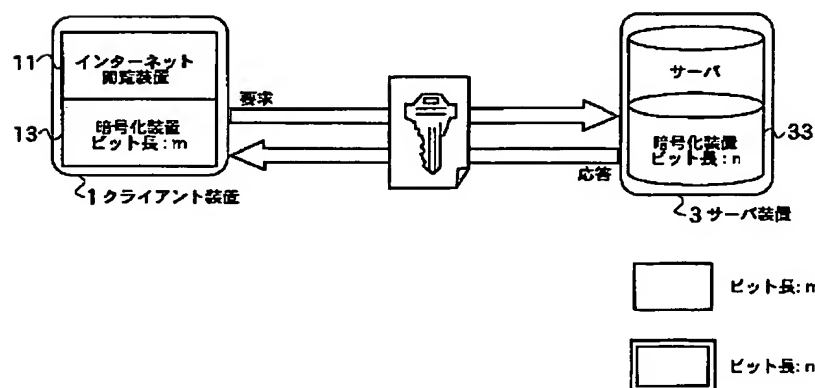
【図3】



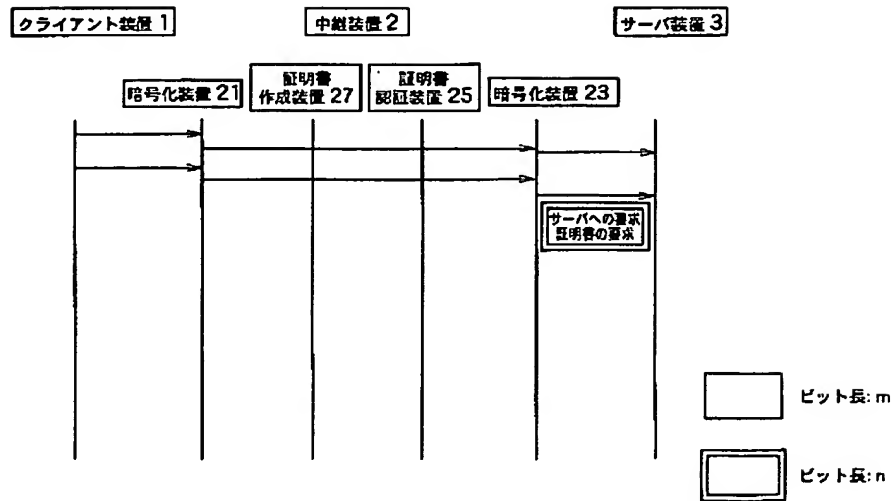
【図4】



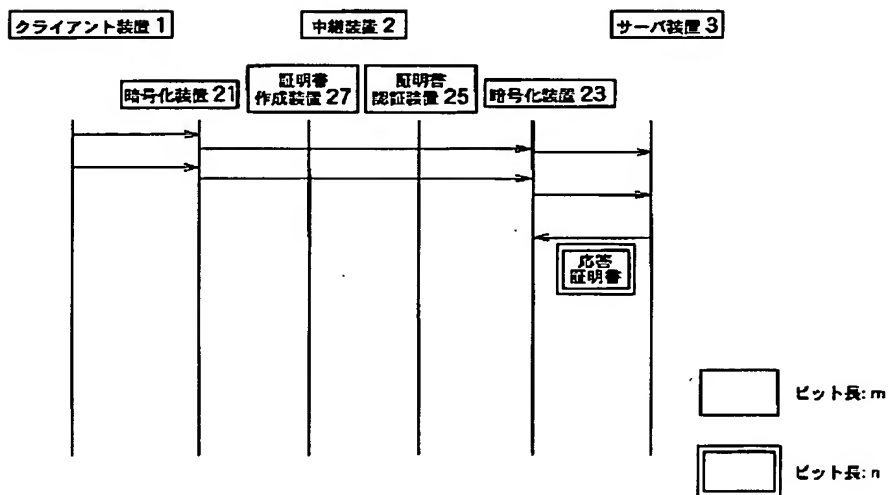
【図19】



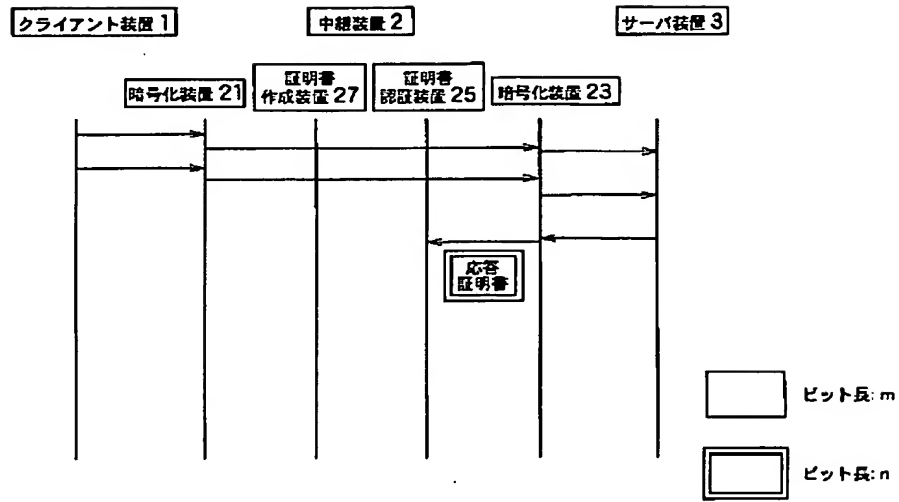
【図 5】



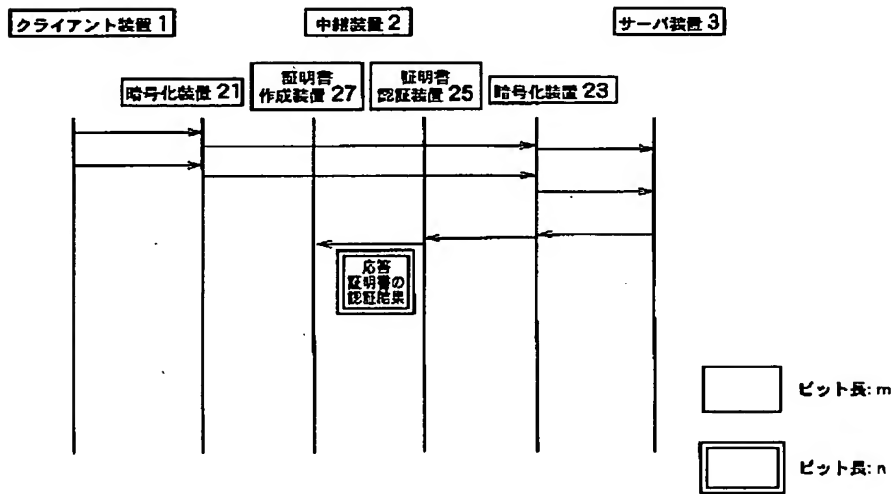
【図 6】



【図 7】



【図 8】



クライアント装置 1

中間装置 2

サーバ装置 3

暗号化装置 21

証明書作成装置 27

証明書検証装置 25

暗号化装置 23

応答新しい証明書

ビット長: m

ビット長: n

クライアント装置 1

中継装置 2

サーバ装置 3

暗号化装置 21

証明書作成装置 27

証明書認証装置 25

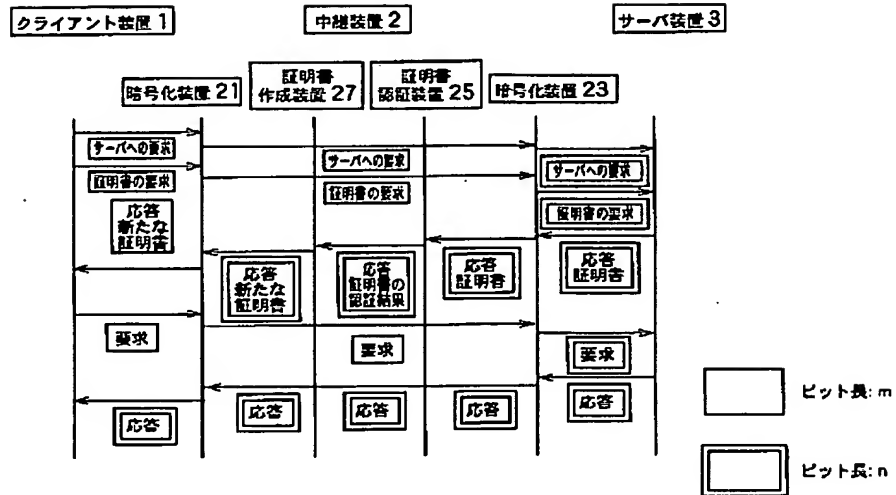
暗号化装置 23

応答
新しい証明書

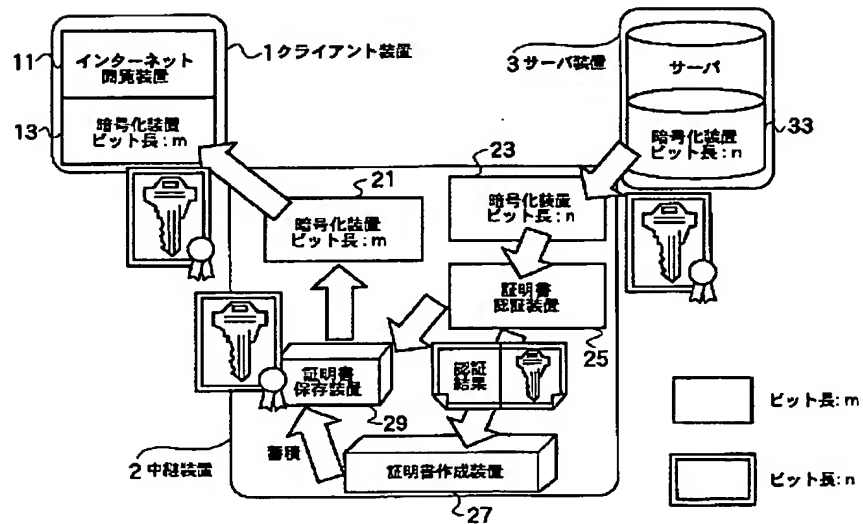
ビット長: m

ビット長: n

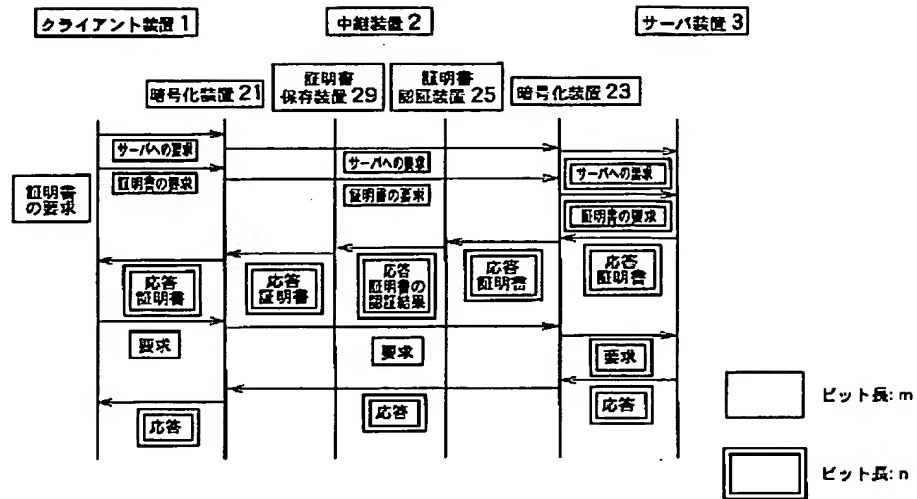
【図11】



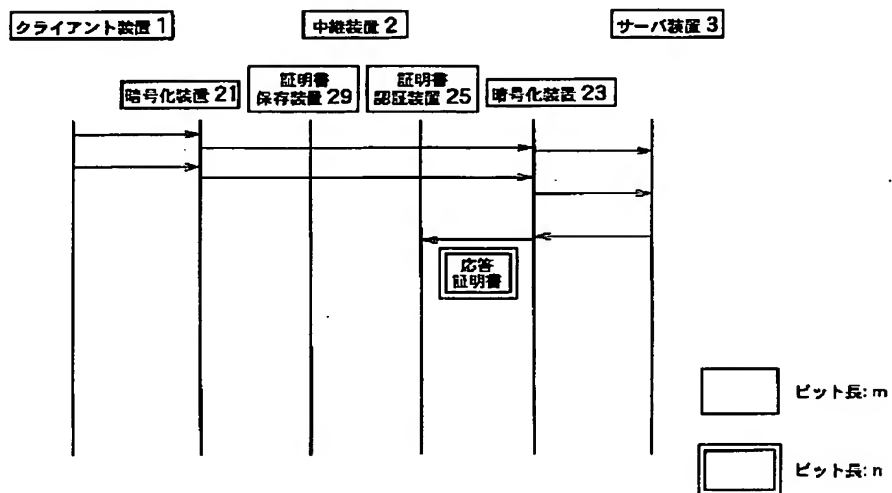
【図12】



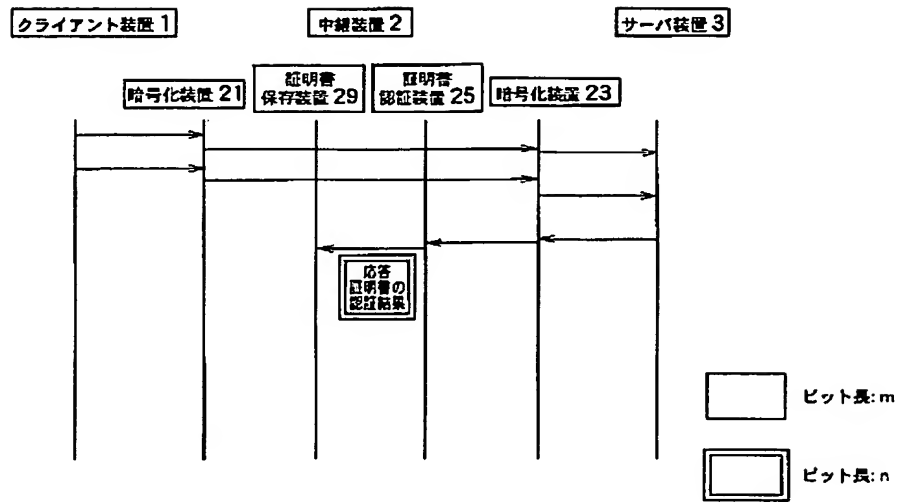
【図13】



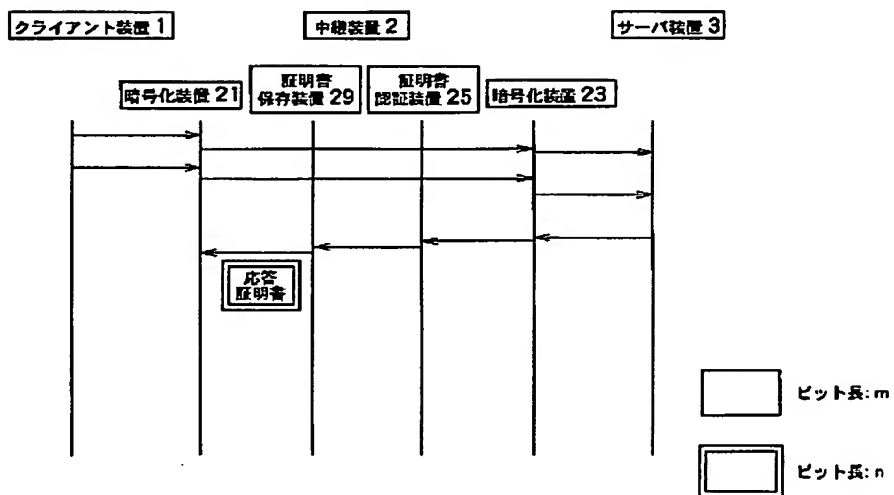
【図14】



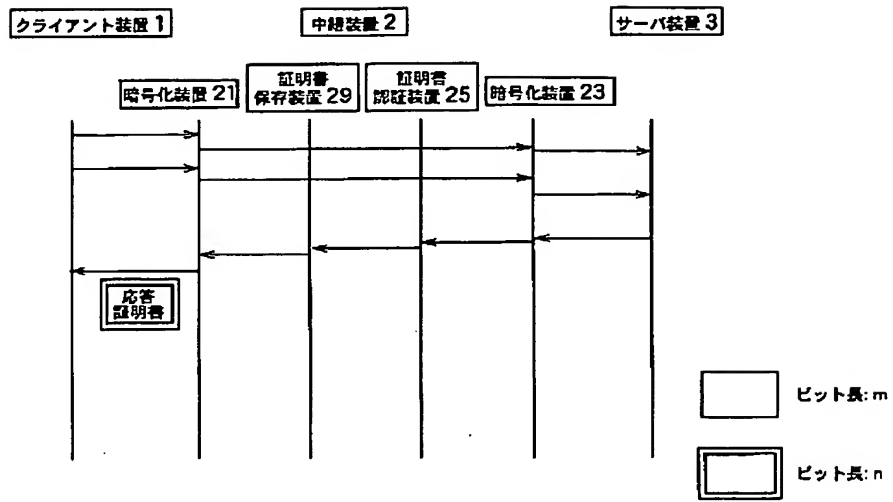
【図15】



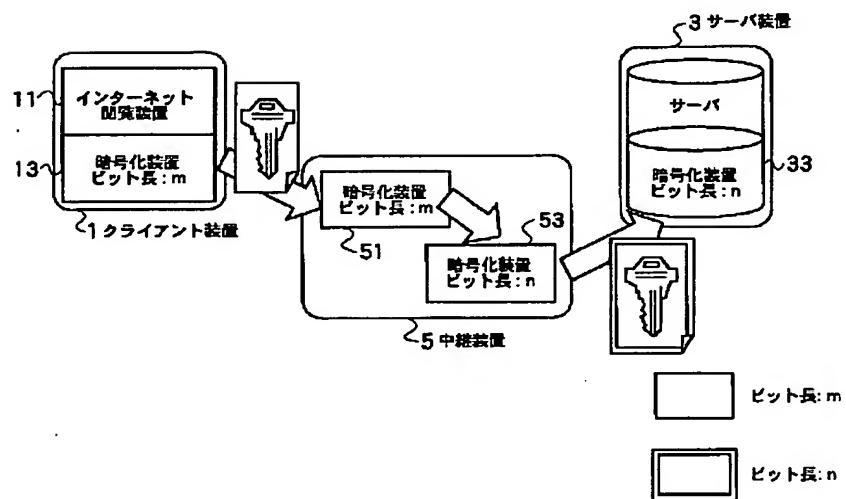
【図16】



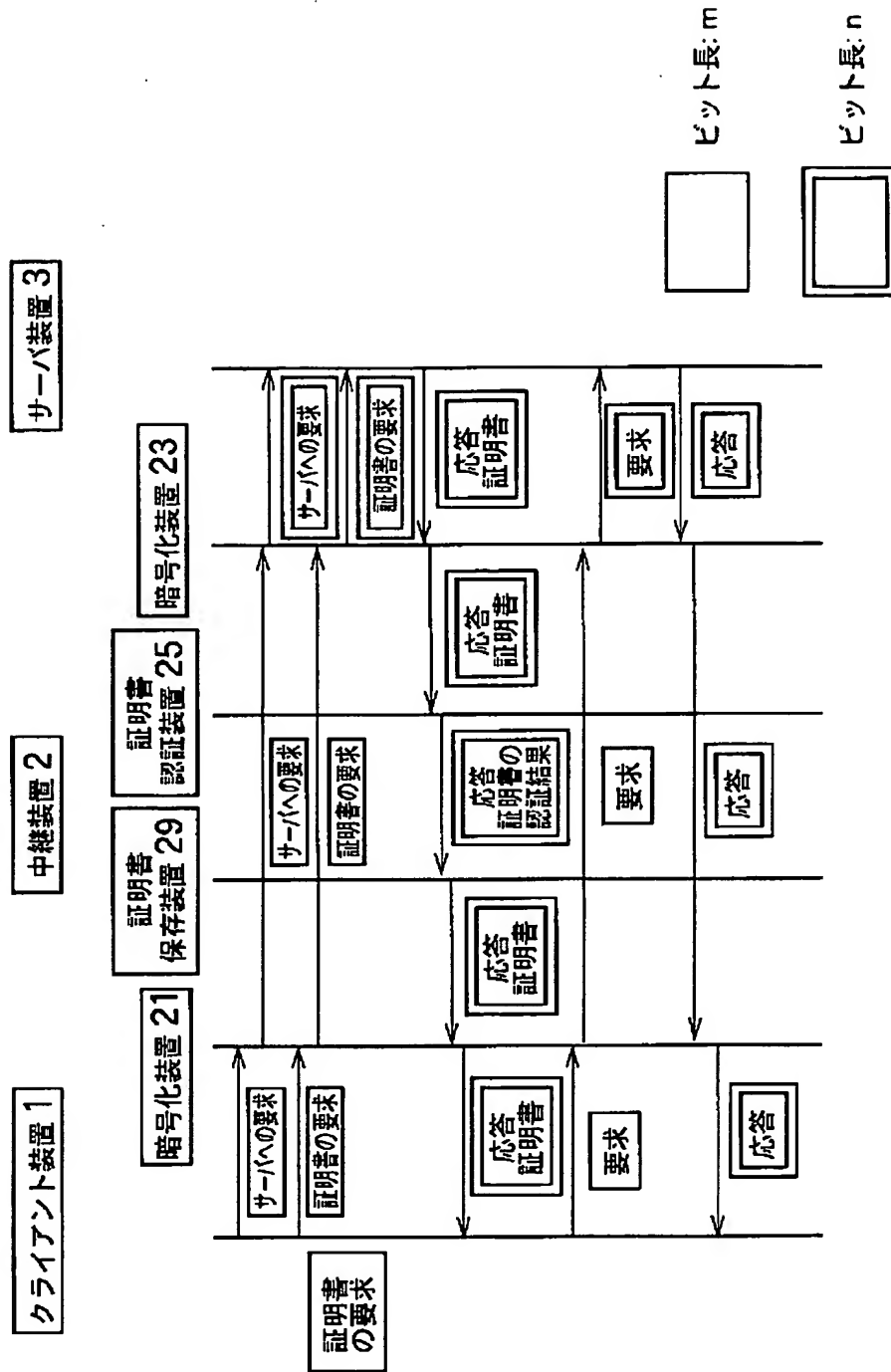
【図17】



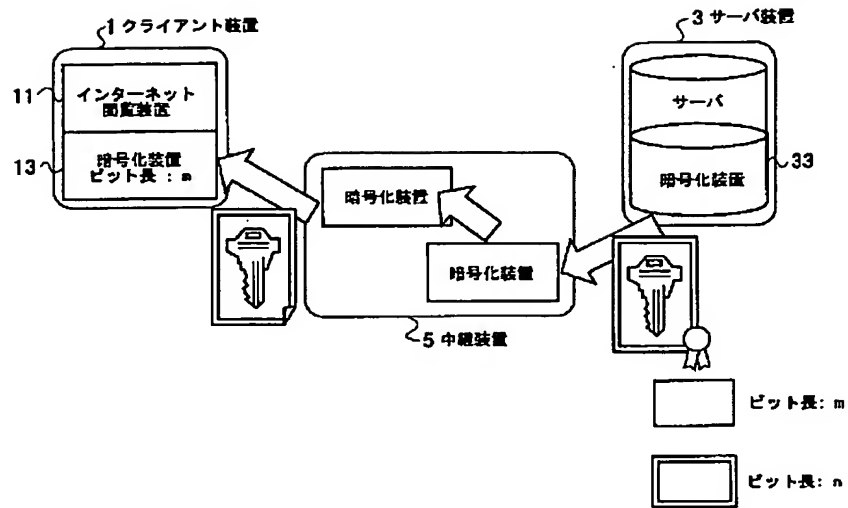
【図20】



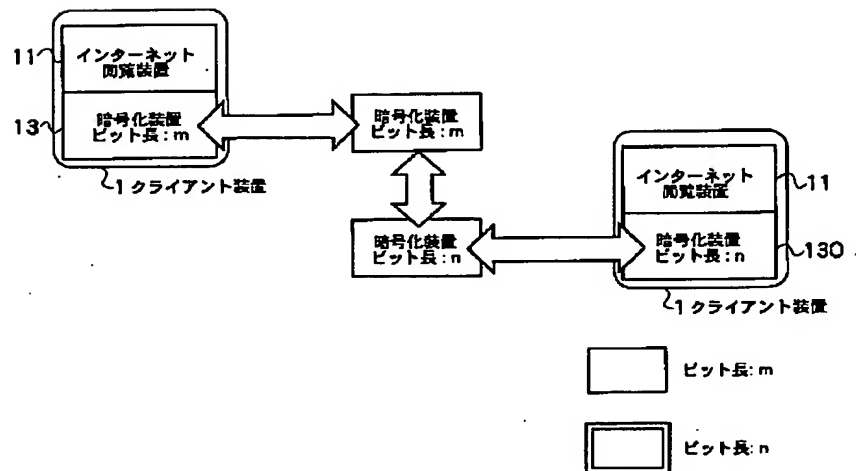
【図18】



【図21】



【図22】



フロントページの続き

Fターム(参考) 5B089 GA11 GA21 JA00 JB23 KA17
 KB13 KC57 KC58 KF05 KH30
 5J104 AA01 AA07 KA01 KA04 LA02
 PA09
 9A001 EE03 JJ25 LL03